ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024
Nos. 24-1113, 24-1130, 24-1183

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC. AND BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

On Petitions for Review of Constitutionality of the
Protecting Americans from Foreign Adversary Controlled Applications Act

---

BRIEF OF *AMICI CURIAE* FORMER CHAIRMAN OF THE FEDERAL COMMUNICATIONS COMMISSION AJIT V. PAI AND FORMER ASSISTANT SECRETARY OF THE TREASURY FOR INVESTMENT SECURITY THOMAS P. FEDDO IN SUPPORT OF RESPONDENT

THOMAS M. JOHNSON, JR.
JEREMY J. BROGGI
MICHAEL J. SHOWALTER
STEPHANIE RIGIZADEH
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
Phone: (202) 719-7000
Fax: (202) 719-7049
tmjohnson@wiley.law
jbroggi@wiley.law
mshowalter@wiley.law
srigizadeh@wiley.law

Counsel for Amici Curiae

August 2, 2024

[caption continued on inside cover]

BRIAN FIREBAUGH, et al.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

BASED Politics Inc.,

Petitioner,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), *amici curiae* state as follows:

A. Parties and *Amici*

Except for the following, the parties, intervenors, and *amici* appearing in this Court in these consolidated cases are listed in the Brief of Petitioners TikTok Inc. and ByteDance Ltd. As of the finalization of this brief, *amici* appearing in this Court in these consolidated cases are Electronic Frontier Foundation; Freedom of the Press Foundation; TechFreedom; Media Law Resource Center; Center for Democracy and Technology; First Amendment Coalition; Freedom to Read Foundation; Cato Institute; Matthew Steilen; Arizona Asian American Native Hawaiian and Pacific Islander for Equity Coalition; Asian American Federation; Asian Americans Advancing Justice Southern California; Calos Coalition; Hispanic Heritage Foundation; Muslim Public Affairs Council; Native Realities; OCA-Asian Pacific American Advocates of Greater Seattle; South Asian Legal Defense Fund; Sikh Coalition; Sadhana; OCA-Asian Pacific American Advocates: San Francisco; Knight First Amendment Institute at Columbia University; Free Press; PEN American Center; Milton Mueller; Timothy H. Edgar; Susan A. Aaronson; Hans Klein; Hungry Panda US, Inc.; Shubhangi Agarwalla; Enrique Armijo; Derek Bambauer; Jane Bambauer; Elettra Bietti; Ashutosh Bhagwat; Stuart N. Brotman; Anupam Chander; Erwin Chemerinsky; James Grimmelmann; Nikolas

Guggenberger; G. S. Hans; Robert A. Heverly; Michael Karanicolas; Kate Klonick; Mark Lemley; David S. Levine; Yvette Joy Liebesman; Dylan K. Moses; Sean O'Brien; and Christopher J. Sprigman.

B. Ruling Under Review

Petitioners seek direct review of the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H (2024). There are no prior rulings under review.

C. Related Cases

These cases were not previously before this Court or any other court. Counsel for *amici curiae* are not aware of any other case currently pending before this or any other court that is related to these cases within the meaning of Circuit Rule 28(a)(1)(C).

August 2, 2024

/s/ Thomas M. Johnson, Jr.
THOMAS M. JOHNSON, JR.
JEREMY J. BROGGI
MICHAEL J. SHOWALTER
STEPHANIE RIGIZADEH
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
Phone: (202) 719-7000
Fax: (202) 719-7049
tmjohnson@wiley.law
jbroggi@wiley.law
mshowalter@wiley.law
srigizadeh@wiley.law

Counsel for Amici Curiae

CIRCUIT RULE 29(D) CERTIFICATE

Amici curiae Ajit V. Pai and Thomas P. Feddo certify that a separate *amicus* brief is necessary. This brief provides the unique perspective of the former Chairman of the Federal Communications Commission and the former Assistant Secretary of the Treasury for Investment Security, who led the interagency Committee on Foreign Investment in the United States. These two former high-ranking government officials have both had personal experience in their respective agencies with the risk posed by People's Republic of China corporate control of American companies that is directly relevant to the issues presented in this appeal.

August 2, 2024

/s/ Thomas M. Johnson, Jr.
Thomas M. Johnson, Jr.
Jeremy J. Broggi
Michael J. Showalter
Stephanie Rigizadeh
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
Phone: (202) 719-7000
Fax: (202) 719-7049
tmjohnson@wiley.law
jbroggi@wiley.law
mshowalter@wiley.law
srigizadeh@wiley.law

Counsel for Amici Curiae

TABLE OF CONTENTS

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES i

CIRCUIT RULE 29(D) CERTIFICATE iii

GLOSSARY xi

INTEREST OF *AMICI CURIAE* 1

STATUTES AND REGULATIONS 3

INTRODUCTION AND SUMMARY 3

ARGUMENT 6

I. Congress's Requirement That TikTok Divest Reflects Legitimate and Longstanding Governmentwide Concerns Over Threats Posed by China's Corporate Ownership. 6

A. TikTok Acknowledges National Security Concerns with China's Corporate Ownership. 7

B. The United States Has Engaged the Threat Posed by China's Corporate Ownership. 9

1. Assessments of Threats Posed by Huawei and ZTE 9

2. The PRC's Cyber and National Intelligence Laws 13

3. The Secure Networks Act and the Covered List 15

4. Section 214 17

C. The United States Has Addressed the Threat Posed by China's Corporate Control Through the CFIUS Process. 19

D. Other Former Government Officials, Politicians, and Academics Agree. 24

II. Viewed In This Light, TikTok's Various Objections to the Divestiture Act Are Misplaced. 27

CONCLUSION.....30

TABLE OF AUTHORITIES

Page(s)

Cases

China Telecom (Americas) Corp. v. FCC,
57 F.4th 256 (D.C. Cir. 2022) 18

Hikvision USA, Inc. v. FCC,
97 F.4th 938 (D.C. Cir. 2024) 16, 29

Holder v. Humanitarian L. Project,
561 U.S. 1 (2010) 8

Huawei Techs. USA, Inc. v. FCC,
2 F.4th 421 (5th Cir. 2021) 2, 11, 28, 29

Huawei Techs. USA, Inc. v. United States,
440 F.Supp.3d 607 (E.D. Tex. 2020) 10, 29

McCulloch v. Maryland,
17 U.S. 316 (1819) 29, 30

Youngstown Sheet & Tube Co. v. Sawyer,
343 U.S. 579 (1952) 29

Constitution, Statutes, and Rules

31 C.F.R. § 800.102 21

47 C.F.R. Part 63 17

47 U.S.C. § 214 17

47 U.S.C. § 1601 note 16

50 U.S.C. §§ 4501–4568 ..... 19, 20

50 U.S.C. § 4502 ..... 19, 20

50 U.S.C. § 4565 ..... 20, 21

Cybersecurity Law of the PRC, ch. III, art. 28, 2017 13

Cybersecurity Law of the PRC, ch. V, art. 51, 2017 13

Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, Title XVII, Subtitle A, § 1702(b)(4), 132 Stat. 1636 (2019).....22

Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 60061 (2020) 23

NDAA for Fiscal Year 2018, Pub. L. No. 115-91, § 1656, 131 Stat. 1283 (2017).....9

NDAA for Fiscal Year 2019, Pub. L. No. 115-232, §§ 889(a), (f)(2)-(3), 132 Stat. 1636 (2018).....9, 10

Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297 (Aug. 14, 2020) 5, 23, 24

Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, §§ 2-4, 134 Stat. 158 (2020).....2, 15

Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021).....2, 16

U.S. Const. art. I, § 8, cl. 3, cl. 18.....29, 30

Executive Branch Materials

Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 6, 2020).....22, 23

In re China Telecom (Americas) Corp., 36 FCC Rcd. 15966 (2021).....17, 18

In re Pacific Networks Corp. and ComNet (USA) LLC, 37 FCC Rcd. 4220 (2022).....19

Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, 36 FCC Rcd. 10578 (2021).....15, 16

Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, 37 FCC Rcd. 13493 (2022).....16

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 34 FCC Rcd. 11423 (2019) (codified at 47 C.F.R. § 54.9).....11

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 35 FCC Rcd. 14284 (2020).....15

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation, 35 FCC Rcd. 6604 (2020).....11, 12, 13

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation, Memorandum Opinion and Order, 35 FCC Rcd. 14435 (2020).....12, 14, 15

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs - ZTE Designation, 35 FCC Rcd. 6633 (2020).....12, 13, 15

Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 9, 2021).....24

Other Authorities

Alexandra G. Neenan et al., *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress*, Cong. Rsch. Serv. (Oct. 6, 2023).....19, 20, 21

Cathleen D. Cimino-Isaacs & Karen M. Sutter, *The Committee on Foreign Investment in the United States*, Cong. Rsch. Serv. (May 17, 2024).....20, 21

CFIUS, Department of Treasury, https://tinyurl.com/fvbyxkrk (last visited Aug. 2, 2024).....20

CFIUS Overview, Department of the Treasury, https://tinyurl.com/3chadfkj (last visited Aug. 1, 2024).....21

Christopher Wray, *2022 Josh Rosenthal Memorial Talk*, University of Michigan (Dec. 2, 2022), https://tinyurl.com/49vw9bhn 26

Colleen McClain, *Majority of Americans say TikTok is a threat to national security*, Pew Research Center (July 10, 2023), https://tinyurl.com/4tp8sd8x 27

International Section 214 Application Filing Guidelines, FCC, https://tinyurl.com/458sudyx (last updated May 14, 2015).....17

James L. Schoff & Asei Ito, *Competing with China on Technology and Innovation*, Carnegie Endowment for International Peace (Oct. 10, 2019), https://tinyurl.com/3jypsf85 .....13, 14

Klon Kitchen, *Ban TikTok Now*, American Enterprise Institute (July 7, 2022), https://tinyurl.com/mwkhz9tb 14

Letter from Chairman Ajit Pai, FCC, to Sen. Tom Cotton (Mar. 20, 2018) 11

Letter from Sen. Tom Cotton et al., to Chairman Ajit Pai, FCC (Dec. 20, 2017) 10, 11

Letter from Sens. Mark Warner & Marco Rubio, to Chairwoman Lina Khan, FTC (July 5, 2022) 25, 26

Letter from the Vandenberg Coalition, to Senate Majority Leader Chuck Schumer and Minority Leader Mitch McConnell (Apr. 10, 2024) 13, 24, 25

Michael Ramsey, *The Constitution's Text in Foreign Affairs* (2007) 30

Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017), https://tinyurl.com/2nnk68j4.....13, 14

Statement of the FTC in the Matter of ByteDance/Musical.ly, (June 18, 2024), https://tinyurl.com/4tc9jxr3 26

Stephen P. Mulligan, *Restricting TikTok (Part I): Legal History and Background*, Cong. Rsch. Serv. (Sept. 28, 2023) 21, 23

Thomas Feddo, *Three Years' Delay to Rein in TikTok*, RealClear Defense (Feb. 15, 2023), https://tinyurl.com/32vbtmse 24

Vandenberg Coalition, *Around the World: Essential Foreign Policy Issues for Leaders*, (Oct. 2022).....24

Vandenberg Coalition, *Myth vs. Fact, Protecting Americans from Foreign Adversary Controlled Applications Act*, (Apr. 10, 2024) 25

Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, FTC (Feb. 27, 2019), https://tinyurl.com/yc3bm84a.....26

Worldwide Threats Assessment: Hearing Before the U.S. Senate Select Committee on Intelligence (Mar. 11, 2024) 26

Yaqiu Wang, *The Problem with TikTok's claim of independence from Beijing*, The Hill (Mar. 24, 2023) 14, 25

GLOSSARY

APA	Administrative Procedure Act
CCP	Chinese Communist Party
CFIUS	Committee on Foreign Investment in the United States
DOJ	Department of Justice
FCC	Federal Communications Commission
FTC	Federal Trade Commission
NDAA	National Defense Authorization Act
PRC	People's Republic of China

INTEREST OF *AMICI CURIAE*

Amici curiae are former high-ranking government officials who oversaw federal regulatory programs with responsibility for reviewing foreign corporate ownership structures of American companies.[1] Through their prior government service, these officials became acutely aware of the national security risks posed by People's Republic of China corporate ownership of companies operating within the United States, including TikTok and other companies in the communications ecosystem.[2] They respectfully submit this brief to highlight the legitimate public policy goals behind the Divestiture Act under review and provide context on similar government programs animated by the same common goal—protecting the vital national security of American citizens.

The Honorable Ajit V. Pai is the former Chairman of the Federal Communications Commission. During his time at the FCC, former Chairman Pai

[1] All parties have consented to the filing of this brief. No party's counsel authored this brief in whole or in part and no party or party's counsel contributed money intended to fund the brief's preparation or submission. The Vandenberg Coalition, a non-partisan network of foreign policy scholars and practitioners who believe in the power of American leadership to protect American national security, contributed to the funding of this brief.

[2] The views expressed in this brief are solely those of *amici* in their personal capacities as former government officials and do not reflect the views of any of their current or prior employers, partners, or employees.

spearheaded a rulemaking that prohibited communications companies that received federal subsidies from purchasing or using equipment from two designated Chinese-owned manufacturers, Huawei and ZTE, and put in place a process for future designations of companies that posed a similar risk to national security. This rulemaking was upheld by the Fifth Circuit. *See Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421 (5th Cir. 2021). This framework, substantially similar to the Divestiture Act, was also ratified by Congress in the Secure Networks Act and expanded in the Secure Equipment Act, which prohibited the FCC from approving for sale in the United States certain equipment produced by the covered manufacturers. *See* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, §§ 2-4, 134 Stat. 158 (2020); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021).

The Honorable Thomas P. Feddo served as the first Assistant Secretary of the Treasury for Investment Security and oversaw the interagency Committee on Foreign Investment in the United States, where he led its national security reviews of several hundred cross-border transactions totaling more than $400 billion. During his stewardship of CFIUS, the Committee undertook a review of the national security risks posed by ByteDance's acquisition of Musical.ly and the integration of TikTok's and Musical.ly's social media applications. That investigation culminated in a presidential order issued by then-President Trump—and kept in effect under

President Biden—finding credible evidence for the President to believe that the acquisition threatened to impair U.S. national security and that ordered ByteDance to divest its interests in TikTok's U.S. operations.

STATUTES AND REGULATIONS

All applicable statutes are contained in Petitioners' briefs.

INTRODUCTION AND SUMMARY

TikTok repeatedly attempts to downplay as "speculative" the national security concerns identified by the Department of Justice that led Congress to adopt the Divestiture Act.[3] Br. Pet'r's TikTok Inc. and ByteDance Ltd. 2, 52-54 ("TikTok Br."). And it criticizes Congress for relying on the "potential" harms TikTok could pose to national security. *Id.* at 18. But TikTok never states that Congress had no legitimate national security reasons to regulate it, nor that the potential threat does not in fact exist. To the contrary, TikTok simply complains that Congress called it out by name in the Act, rather than according it additional procedural protections, and that it ordered divestiture as opposed to alternate measures TikTok considered sufficient. According to TikTok, when Congress regulates a communications platform, that violates the First Amendment.

[3] Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 895, 955-60 (2024) ("Divestiture Act").

But the policies and approach reflected in the Divestiture Act are nothing new or extraordinary. Congress frequently makes judgments that specific foreign companies pose a national security threat, while putting in place a process to allow the Executive Branch to identify additional threats that materialize in the future. In recent years, Congress has done this repeatedly in the communications space to address the threats posed by PRC corporate ownership of American companies. That threat is endemic to PRC law, which requires companies owned by China's citizens to permit state-authorized covert surveillance into data collected by the company.

In the case of TikTok, that could mean the exposure of millions of Americans' sensitive personal information. TikTok does not deny this is how PRC law operates; it simply believes its own negotiated restrictions would be preferable to divestiture. But it is ludicrous to suggest, as TikTok does, that the U.S. Government cannot prefer divestiture as a policy option, or that it must wait for Americans to be compromised before it can act. To the contrary, over the past 50 years Congress and the Executive Branch have developed and augmented an interagency national security process through CFIUS—rooted in the President's constitutional Commander in Chief authorities, and chaired on his behalf by the Secretary of the Treasury—that may ultimately use divestiture as a tool to resolve national security risks. These national security tools were most recently overhauled and enhanced in

2018, in substantial part because of the risks posed to the United States and its people by the PRC. During the Trump Administration, CFIUS initiated an investigation into a ByteDance acquisition that led the President to issue a presidential order concluding that ByteDance must divest its interests in TikTok's U.S. operations. *See Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297 (Aug. 14, 2020). That order, which remains on the books even following a change in administrations, now should be considered to represent the bipartisan judgment of two U.S. presidents.

If this Court accepted TikTok's arguments, it would potentially imperil the operation of longstanding statutory national security review processes that deem a specific foreign-controlled company to pose a U.S. national security threat as a result of the company acquiring or seeking to acquire specific American businesses and their assets. A company should not be able to use the mere fact that it engages in expressive activity to invoke the First Amendment to avoid both Congress's and the Executive Branch's considered judgment that its corporate structure and its relation to an adversary of the United States poses an unacceptable risk to U.S. national security.

ARGUMENT

I. Congress's Requirement That TikTok Divest Reflects Legitimate and Longstanding Governmentwide Concerns Over Threats Posed by China's Corporate Ownership.

Across government branches and the political spectrum, American leaders and policymakers have long expressed serious concern about the national security threat posed by the Chinese government through corporate ownership of American companies. Indeed, as TikTok acknowledges, before the Divestiture Act was enacted, DOJ informed Congress of its serious national security concerns surrounding TikTok itself. For years, the federal entities previously overseen by *amici* (the FCC and CFIUS) have recognized that China's control of companies operating in the U.S. can manifest threats from the CCP and Chinese government and have worked to mitigate such risks through concrete action and the exercise of their respective authorities. Congress too has frequently articulated these risks—including through committee hearings, congressional reports and letters, and congressional enactments that identify specific companies posing such acute threats. These concerns are unrelated to any speech by these companies or their customers. The Divestiture Act is yet another such preventative measure, reflecting the same concerns about significant U.S. national security risks.

A. TikTok Acknowledges National Security Concerns with China's Corporate Ownership.

As TikTok acknowledges, "before Congress passed the Act, the Justice Department provided members of Congress a one-page document describing 'key national security concerns.'" TikTok Br. 18. TikTok dismisses these concerns as mere "speculative" or "potential" threats, but that framing cannot withstand scrutiny.

As DOJ explained, TikTok "collects tremendous amounts of sensitive data." *Id.* This matters because the Chinese government "could use TikTok to access data on millions of U.S. users and control the software on millions of U.S. devices." TikTok App. 156. The Chinese government also "leads the world in using surveillance and censorship to keep tabs on its population, repress dissent, and counter perceived threats abroad." *Id.* And the Chinese government requires companies doing business in China (like ByteDance) to share their data with the government. *Id.* That data sharing is done secretly—there is no way for the United States to know when or how much data is being shared. *Id.* And indeed U.S. media has reported that ByteDance employees in China have repeatedly used TikTok to access U.S. user data and track American journalists. *Id.* The Chinese government's "ability to weaponize data and conduct sophisticated influence campaigns," DOJ warned, "will only advance over time" and will "be difficult to detect." *Id.*

Considering this threat, DOJ concluded that legislation must "separate TikTok the company from Beijing and its PRC-based parent company." *Id.*

TikTok never denies any of DOJ's assertions, but instead complains that DOJ did not present hard evidence that the threats it discussed have yet been realized. *See* TikTok Br. 52-53. But that is incorrect—DOJ identified reporting that ByteDance employees already have used TikTok to spy on Americans and American journalists. TikTok App. 156. And more importantly, the U.S. Government may take preventative measures to protect its citizens from foreign threats before they become realized harms. It would be a "dangerous requirement" to "demand[] hard proof—with 'detail,' 'specific facts,' and 'specific evidence'" in this context, where "national security and foreign policy concerns arise in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess." *Holder v. Humanitarian L. Project*, 561 U.S. 1, 34-35 (2010).

As *amici curiae* know well from their prior government service, DOJ's concerns are well founded. The United States has long had significant and legitimate public policy concerns over PRC-based corporate control of businesses in the United States generally—and more recently, with TikTok in particular. Under then-Chairman Pai, the FCC recognized the threat posed by China's corporate ownership and combatted this threat through a series of rulemakings undertaken in interbranch

dialogue with Congress. And during Assistant Secretary Feddo's tenure, CFIUS also took concrete steps to address that threat, and specifically the threat posed by ByteDance's ownership and control of the U.S. business.

B. The United States Has Engaged the Threat Posed by China's Corporate Ownership.

During Chairman Pai's administration, the FCC worked alongside Congress to identify and address a series of threats to national security posed by China's control of corporations owned by its citizens. This has sometimes included identifying specific companies that presented national security risks and naming them for particularized treatment. The resulting legislative and regulatory programs have been uniformly upheld by courts.

1. Assessments of Threats Posed by Huawei and ZTE

In the 2018 National Defense Authorization Act, Congress barred the Department of Defense from using telecommunications equipment or services produced or provided by China's Huawei and ZTE for certain federal programs. NDAA for Fiscal Year 2018, Pub. L. No. 115-91, § 1656, 131 Stat. 1283, 1762 (2017). Then, in the 2019 NDAA, Congress prohibited Executive Branch agencies from using federal funds to procure equipment that use "covered telecommunications equipment." NDAA for Fiscal Year 2019, Pub. L. No. 115-232, §§ 889(a), (f)(2)-(3), 132 Stat. 1636, 1918 (2018). The 2019 NDAA defines

"covered telecommunications equipment or services" in four categories, one of which specifically names PRC-based companies Hikvision, Dahua, and Hytera to encompass their equipment. *See id.* § 889(f)(3)(B). Apart from these specific designations, the NDAA provides a process through which certain national security authorities could identify other companies' equipment that posed a threat to the United States. *See id.* § 889(a), (f)(3)(D). In this, the NDAA mirrored in form the Divestiture Act; Congress had sufficient information to designate specific companies as threats, but established a process to allow the federal government to expand that list as threats evolved. Huawei challenged that specific designation as an unlawful Bill of Attainder, among other things, but the statute was upheld. *See Huawei Techs. USA, Inc. v. United States*, 440 F.Supp.3d 607 (E.D. Tex. 2020).

In 2017, around the time the first NDAA was adopted, Senator Tom Cotton and colleagues wrote a letter to then-Chairman Pai alerting the FCC of the national security risk that would arise if U.S. telecommunications providers began selling Huawei consumer products without modifications. Letter from Sen. Tom Cotton et al., to Chairman Ajit Pai, FCC (Dec. 20, 2017). The Senators emphasized that Congress had "long been concerned about Chinese espionage in general, and Huawei's role in that espionage in particular." *Id.* Citing a 2013 House Permanent Select Committee on Intelligence report, the Senators underscored "Huawei's ties to the Chinese Communist Party, as well as to Chinese intelligence and security

services." *Id.* Then-Chairman Pai responded that he shared these "concerns about the security threat that Huawei and other Chinese technology companies pose to our communications networks," and would "take proactive steps" in this matter. Letter from Chairman Ajit Pai, FCC, to Sen. Tom Cotton (Mar. 20, 2018).

In response, the FCC proposed a rule prohibiting the use of subsidies from the FCC's Universal Service Fund to purchase or obtain equipment or services from a provider identified as posing a national security risk to the communications networks. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 34 FCC Rcd. 11423, ¶ 26 (2019) (codified at 47 C.F.R. § 54.9) ("Initial Huawei Order"). In that proposal, the Commission initially designated Huawei and ZTE as likely to pose a national security threat, and established a process for the FCC's Public Safety and Homeland Security Bureau to designate additional companies. *Id.* ¶¶ 27, 64. Huawei challenged the FCC's constitutional and statutory authority to adopt this regime, as well as its initial designation without additional process. But here too, a court ruled the FCC's framework was lawful. *See Huawei*, 2 F.4th at 427.

Following additional public comment, the FCC issued final designation orders excluding Huawei and ZTE as permissible suppliers for companies participating in Universal Service Fund programs. With respect to Huawei, the FCC determined that "Huawei pose[d] a national security threat to our nation's communications

networks and the communications supply chain." *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, 35 FCC Rcd. 6604, ¶ 10 (2020) ("Huawei Final Designation Order"). The Public Safety and Homeland Security Bureau issued a rule designating Huawei and its American affiliate as national security risks and barring recipients of federal subsidies administered by the FCC under its Universal Service Fund from using the funds to purchase their equipment. *Id.* ¶ 1. The full Commission affirmed the Bureau's findings, concluding that Huawei is "'a unique threat' to the security and integrity of the nation's communications networks and communications supply chain because of its size, close ties to the Chinese government, and security flaws identified in its equipment." *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, Memorandum Opinion and Order, 35 FCC Rcd. 14435, ¶ 6 (2020) ("Commission Review of Huawei Final Designation Order").

Similarly, the FCC designated ZTE as "a national security threat to our nation's communications networks and communications supply chain." *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs - ZTE Designation*, 35 FCC Rcd. 6633, ¶ 9 (2020) ("ZTE Final Designation Order"). The FCC noted "ZTE's close ties to the Chinese government and obligations under Chinese law" and its "disregard for U.S. national security

laws." *Id.* ¶ 11. And the FCC found that "ZTE poses a particular security risk because Chinese intelligence agencies have opportunities to tamper with its products in both the design and manufacturing processes." *Id.* ¶ 13.

2. The PRC's Cyber and National Intelligence Laws

The FCC's findings in the Huawei and ZTE Final Designation Orders relied in part on the threat posed generally by China's corporate control, which is in part the product of PRC laws that compel cooperation with the CCP. Huawei Final Designation Order ¶¶ 12-14, 18-27; ZTE Final Designation Order ¶¶ 11-18. China's Cybersecurity Law, for example, requires China-controlled companies to provide direct access to their data and threatens penalties, including arrest, for failure to comply. Article 28 requires China's internet companies to assist the government in "protecting national security and investigating crimes." Cybersecurity Law of the PRC, ch. III, art. 28, 2017; *see also* Letter from the Vandenberg Coalition, to Senate Majority Leader Charles Schumer and Minority Leader Mitch McConnell (Apr. 10, 2024) ("Vandenberg Letter"). Article 51, in turn, allows China to "establish a cybersecurity monitoring, early warning, and information communication system," which internet companies would be required to implement. Cybersecurity Law of the PRC, ch. V, art. 51, 2017. And a separate law, Beijing's 2017 National Intelligence Law, creates "affirmative legal responsibilities for Chinese firms to provide access, cooperation, or support for Beijing's intelligence-gathering

activities." James L. Schoff & Asei Ito, *Competing with China on Technology and Innovation*, Carnegie Endowment for International Peace (Oct. 10, 2019), https://tinyurl.com/3jypsf85; *see* Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017), https://tinyurl.com/2nnk68j4.

China's national security and data-security laws apply extraterritorially to its companies no matter where they operate, and include the operations of any foreign subsidiaries, such as TikTok U.S. That means that a China-controlled company or subsidiary (including TikTok U.S.) must share with the CCP any data that it collects, no matter where it is collected or stored. *See* Klon Kitchen, *Ban TikTok Now*, American Enterprise Institute (July 7, 2022), https://tinyurl.com/mwkhz9tb. And the CCP "has a record of making private Chinese companies carry out its political deeds, including censoring and surveilling Americans." Yaqiu Wang, *The Problem with TikTok's claim of independence from Beijing*, The Hill (Mar. 24, 2023), https://tinyurl.com/ycxabvfm.

In the Huawei and ZTE Final Designation Orders, the FCC unanimously recognized the risks created by these laws. In the Huawei proceeding, the FCC observed that the "National Intelligence Law grants the Chinese government the power to compel Huawei to assist it in espionage activities," Commission Review of Huawei Final Designation Order ¶ 16 (citations omitted), and that companies

largely cannot refuse the Chinese government's requests. *Id.* ¶¶ 15-17. In the ZTE proceeding, similarly, the FCC emphasized that "[a] close reading of the provisions of the Chinese National Intelligence Law demonstrates that it is broad enough to allow the Chinese government to compel Chinese companies such as ZTE to assist it in its espionage activities." ZTE Final Designation Order ¶ 17.

3. The Secure Networks Act and the Covered List

In March 2020, Congress enacted the Secure Networks Act, which requires the FCC to maintain a list of "covered communications equipment and services" that pose a national security risk and prohibits the use of FCC-administered federal funds on covered equipment or services. Secure and Trusted Communications Networks Act of 2019, §§ 2-4. This "Covered List" must include equipment that is "covered telecommunications equipment" under Section 889(f)(3) of the 2019 NDAA. *Id.* § 2(c)(3). The 2019 NDAA, to repeat, names Dahua, Hikvision, and Hytera specifically.

In December 2020, the FCC issued an order to implement the Secure Networks Act. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd. 14284 (2020). The FCC stated that the Covered List would include certain video surveillance and telecommunications equipment produced by Hikvision, Dahua, and Hytera. *Id.* ¶ 68. Then, in June 2021, the FCC proposed a rule effectively banning

the importation, sale, or marketing of Covered List equipment. *See Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, 36 FCC Rcd. 10578 (2021). The FCC explained that its proposed measures would serve the public interest by addressing significant national security risks, consistent with the Commission's statutory duty to safeguard "the national defense" and "promot[e] safety of life and property." *Id.* ¶¶ 6, 65 (citing 47 U.S.C. § 151).

While the Commission's rulemaking was ongoing, Congress enacted the Secure Equipment Act, which ratified the FCC's rule by directing the FCC to clarify that it would "no longer review or approve any application for equipment authorization for equipment that is on the [Covered List]." 47 U.S.C. § 1601 note; Secure Equipment Act of 2021, 135 Stat. 423 (2021). In November 2022, the FCC issued an order fulfilling that directive. *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, 37 FCC Rcd. 13493, ¶¶ 39, 42-43 (2022). This Court upheld that order in relevant part, recognizing that "Congress has clearly expressed its view that [Hikvision's and Dahua's] products pose a risk to national security" and that "the national-security judgments and concerns underlying the Executive Branch's decision in this case counsel deference." *See Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 945, 948 (D.C. Cir. 2024).

4. Section 214

Another way the FCC has confronted the threat posed by China's corporate influence is through its enforcement of Section 214 of the Communications Act. Section 214 outlines the requirements for telecommunications carriers seeking to construct, acquire, operate, or discontinue facilities or services. *See* 47 U.S.C. § 214. Carriers must submit an application to the FCC that provides detailed information about the proposed action, and the FCC evaluates whether the proposed action serves the public interest, convenience, and necessity. *See id.* The FCC has promulgated filing guidelines for international Section 214 applications, which apply to companies seeking to provide U.S.-international telecommunications service. *See generally* 47 C.F.R. Part 63. Any company that has received FCC authorization to provide U.S.-international telecommunications service must obtain prior Commission approval before consummating a substantial transfer of control or assigning Section 214 authorization to any other company. *See id.* § 63.24; *International Section 214 Application Filing Guidelines*, FCC, https://tinyurl.com/458sudyx (last updated May 14, 2015).

Then-Chairman Pai acted against China Telecom under Section 214, with a unanimous FCC revoking its domestic and international Section 214 authority due to national security concerns. *In re China Telecom (Americas) Corp.*, 36 FCC Rcd. 15966, ¶¶ 1-14, 65 (2021). China Telecom, the FCC found, was "subject to

exploitation, influence, and control by the Chinese government" and was "highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight." *Id.* ¶¶ 2, 44. The FCC also determined that China Telecom's services provide the company "with access to U.S. telecommunications infrastructure and U.S. customer records," opportunities to "access [and] disrupt U.S. communications," and "the opportunity to facilitate espionage and other activities harmful to the interests of the United States." *Id.* ¶ 68.

This Court rejected a challenge to that order, deferring to the FCC's expertise and citing the same national security concerns underlying the Divestiture Act. "China has augmented the level of state control over the cyber practices of Chinese companies," the Court explained, and recent laws "require[] Chinese companies to cooperate with state agencies on cybersecurity supervision and inspection." *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 263 (D.C. Cir. 2022). "The Office of the Director of National Intelligence now warns of cyberattacks by the Chinese government and the potential use of Chinese information technology firms as systemic espionage platforms." *Id.* at 262-63. "The FBI [likewise] warns that no country poses a broader, more severe intelligence collection threat than China." *Id.* at 263.

The FCC also revoked the Section 214 domestic and international authority of Pacific Networks Corporation and its subsidiary. *In re Pacific Networks Corp. and ComNet (USA) LLC*, 37 FCC Rcd. 4220, ¶¶ 1-2 (2022). As with China Telecom, the FCC determined that the companies were "subject to exploitation, influence, and control by the Chinese government and are highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight." *Id*. ¶¶ 2, 44-45. The Commission also found that the companies' "access to U.S. telecommunications infrastructure and sensitive U.S. consumer information" facilitated "numerous opportunities to access, monitor, store, and in some cases disrupt and/or misroute U.S. communications." *Id*. ¶ 74.

C. The United States Has Addressed the Threat Posed by China's Corporate Control Through the CFIUS Process.

CFIUS, established by President Ford in a 1975 Executive Order, is associated with the Defense Production Act, which equips the President with certain authorities over domestic industry and empowers him in matters of national security. *See* 50 U.S.C. §§ 4501-4568; Alexandra G. Neenan et al., *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress* at 1, Cong. Rsch. Serv. (Oct. 6, 2023). In the Act, Congress declared that "the security of the United States is dependent on the ability of the domestic industrial base to supply materials and services for the national defense and to prepare for and respond to military conflicts,

natural or man-caused disasters, or acts of terrorism." 50 U.S.C. § 4502(1). Specifically, the Act "provides the President with an array of authorities to shape national defense preparedness programs and to take appropriate steps to maintain and enhance the domestic industrial base." 50 U.S.C. § 4502(4).

Notably, the Defense Production Act extends beyond military preparedness to broadly safeguarding Americans from threats and emergencies. *See* 50 U.S.C. §§ 4501-4568; *see* Neenan et al., *supra*, at 1, 4. For example, the Act enables the President to act on, among other things, mergers, acquisitions, or takeovers "by or with any foreign person that could result in foreign control of any United States business" and "that threaten[] to impair the national security of the United States." 50 U.S.C. §§ 4565(a)(4)(B)(i), (d).

CFIUS is an interagency committee chaired by the Secretary of the Treasury that assists the President in carrying out certain national security-related obligations under the Defense Production Act, facilitating the President's oversight of potential national security risks that arise from certain transactions involving foreign direct investment in U.S. businesses. *See* 50 U.S.C. § 4565(k); *CFIUS*, Department of Treasury, https://tinyurl.com/fvbyxkrk (last visited Aug. 2, 2024); Cathleen D. Cimino-Isaacs & Karen M. Sutter, *CFIUS* at 1, Cong. Rsch. Serv. (May 17, 2024); Neenan et al., *supra*. In particular, CFIUS reviews and investigates whether foreign investment transactions could "impair U.S. national security," for example, giving

foreign government access to, or influence over, cutting-edge U.S. technology, key infrastructure, or sensitive data about U.S. persons. *See* Neenan et al., *supra*, at 17; Cimino-Isaacs & Sutter, *supra*. CFIUS jurisdiction includes the review of mergers, acquisitions, and takeovers that could result in foreign control of a U.S. business; certain noncontrolling investments in businesses involved in critical technologies, critical infrastructure, or sensitive personal data; and certain real estate transactions. *See* Neenan et al., *supra*, at 17; 50 U.S.C. § 4565.

CFIUS can clear or suspend a transaction, refer a transaction to the President, or enter into or impose deal conditions or requirements "to mitigate any risk to the national security of the United States that arises as a result of the covered transaction." 50 U.S.C. § 4565(l)(1)-(3); *see* Stephen P. Mulligan, *Restricting TikTok (Part I): Legal History and Background*, Cong. Rsch. Serv. (Sept. 28, 2023); *CFIUS Overview*, Department of the Treasury, https://tinyurl.com/3chadfkj (last visited Aug. 1, 2024). CFIUS's decision to pursue one of these options stems from "a risk-based analysis ... of the effects on the national security of the United States of the covered transaction." 31 C.F.R. § 800.102. This analysis involves the evaluation of three key elements: the potential threat posed by the foreign investor or acquirer; national security vulnerabilities manifested through the U.S. business; and consequences to U.S. national security that could arise "from the exploitation of the vulnerabilities by the threat actor." 31 C.F.R. § 800.102(a)-(c). Identifying, and

then resolving and eliminating, national security risk is the foundation of the CFIUS mission.

Former Assistant Secretary Feddo oversaw the implementation of a congressional directive to modernize CFIUS and expand its authorities under the bipartisan Foreign Investment Risk Review Modernization Act of 2018. Congress found that "the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security, which warrants an appropriate modernization of the processes and authorities of" CFIUS. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, Title XVII, Subtitle A, § 1702(b)(4), 132 Stat. 1636 (2019).

Also under Assistant Secretary Feddo's leadership, CFIUS scrutinized ByteDance's 2017 acquisition of Musical.ly, a popular social media application, which was acquired by ByteDance and merged with its TikTok application. On or around late 2019, CFIUS undertook an investigation of ByteDance's acquisition to assess the national security risks arising from the transaction, including the potential for U.S. user data access by the PRC government.

Separate from the CFIUS authorities, in early August 2020 then-President Trump issued an Executive Order under the International Emergency Economic Powers Act, to address national security threats posed by TikTok. Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 6, 2020). He observed TikTok's data collection

"threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." *Id.* As a result of this Executive Order, the Secretary of Commerce prohibited certain transactions with TikTok, such as the provision of content delivery network and hosting services. *Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 60061 (2020); *see* Mulligan, *supra*.

Shortly thereafter, on August 14, 2020, following CFIUS's referral of its national security assessment of the ByteDance acquisition to the President, President Trump invoked his authority under both the Constitution and the Defense Production Act to order ByteDance to divest "all interests and rights in any tangible or intangible assets or property" of TikTok in the United States. *See Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297. He further ordered the divestment of all interests and rights in "any data obtained or derived from TikTok application or Musical.ly application users in the United States." *Id.* In justifying these actions and others regarding TikTok in the United States, the President cited

to "credible evidence" that ByteDance could "take action that threatens to impair the national security of the United States." *Id.*

After a change in Administrations, President Biden on June 9, 2021, revoked the August 6, 2020 Executive Order but, to date, has kept in effect the August 14, 2020 presidential order requiring divestment of TikTok's U.S. assets and U.S. person data. *See* Thomas Feddo, *Three Years' Delay to Rein in TikTok*, RealClear Defense (Feb. 15, 2023), https://tinyurl.com/32vbtmse; *Protecting Americans' Sensitive Data from Foreign Adversaries*, Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 9, 2021). The national security concern about TikTok, therefore, is the "considered judgment of two presidents." Feddo, *supra*. And over the course of these two presidencies, "TikTok has only grown in influence and further insinuated itself into American life." *Id.*

D. Other Former Government Officials, Politicians, and Academics Agree.

Other former government officials and academics share *amici curiae*'s concerns about PRC corporate ownership and the magnitude of the threat it poses to national security. The Vandenberg Coalition, a group that includes many former high-ranking government officials, has argued that the CCP represents perhaps the greatest threat to United States national security. *See* Vandenberg Coalition, *Around the World: Essential Foreign Policy Issues for Leaders* at 1, (Oct. 2022). For

example, the "CCP has purchased American farmland and infrastructure near military bases for espionage purposes," "advanced China's military and technological capabilities through intellectual property theft," and "catalyzed America's synthetic opioid crisis by flooding our country with fentanyl." Vandenberg Letter. The Vandenberg Coalition estimates that China's theft of American intellectual property costs the United States around $600 billion every year. *See* Vandenberg Coalition, *Myth vs. Fact, Protecting Americans from Foreign Adversary Controlled Applications Act* at 1, (Apr. 10, 2024).

TikTok is a particularly effective tool for the CCP to achieve its geopolitical objectives. China's corporate control makes TikTok in particular "extremely vulnerable to CCP demands." Wang, *supra*. As the Vandenberg Coalition has explained, companies "must comply" with PRC "government requests [for] company data, networks, or related information." Vandenberg Letter. And ByteDance is no exception. *Id.* In short, China's industry and the CCP work together to reach CCP-determined goals. *See* Final Brief for FCC and United States at 76, *Huawei Techs. USA, Inc. v. FCC*, No. 19-60896 (5th Cir. 2020) (describing government authorities' belief that China significantly threatens national security).

Recognizing the danger, in 2022 Democratic Senator Mark Warner and Republican Senator Marco Rubio sent a letter to the Federal Trade Commission expressing concerns over China's collection of Americans' data through TikTok.

Letter from Sens. Mark Warner & Marco Rubio, to Chairwoman Lina Khan, FTC (July 5, 2022). This came after TikTok previously settled with the FTC to pay $5.7 million over allegations that the company illegally collected personal information from children. *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, FTC (Feb. 27, 2019), https://tinyurl.com/yc3bm84a. And just this summer, the FTC referred a new complaint to DOJ indicating new or ongoing TikTok violations of data-privacy practices. *Statement of the FTC in the Matter of* ByteDance/Musical.ly, (June 18, 2024), https://tinyurl.com/4tc9jxr3.

FBI Director Christopher Wray similarly explained before Congress that ByteDance "is, for all intents and purposes, beholden to the CCP." Worldwide Threats Assessment: Hearing Before the U.S. Senate Select Committee on Intelligence (Mar. 11, 2024). He explained that the CCP "influence operation" is "extraordinarily difficult to detect, which is part of what makes the national security concerns represented by TikTok so significant." *Id.* Director Wray also recently explained that TikTok allows the Chinese government to "manipulate content" and "collect data through [TikTok] on users which can be used for traditional espionage operations." Christopher Wray, *2022 Josh Rosenthal Memorial Talk*, University of Michigan (Dec. 2, 2022), https://tinyurl.com/49vw9bhn.

The public shares these concerns. According to a 2023 Pew Research Center survey, most Americans believe that TikTok is a national security threat and are concerned about TikTok's data collection practices. Colleen McClain, *Majority of Americans say TikTok is a threat to national security*, Pew Research Center (July 10, 2023), https://tinyurl.com/4tp8sd8x.

II. Viewed In This Light, TikTok's Various Objections to the Divestiture Act Are Misplaced.

Because the Divestiture Act targets the serious national security threats that TikTok poses, TikTok's attempt to mischaracterize how the Act operates and what it is designed to accomplish fails.

TikTok argues that the Act "discriminate[s] based on speaker and content." TikTok Br. 4. But the Act does no such thing. Rather, the Act targets ByteDance's conduct and is based on the government's longstanding concerns about that conduct. The Act fits comfortably alongside the existing regulatory structures discussed in this brief that similarly aim to tackle evolving national security risk.

The Act does not regulate speech based on "who the speaker is and what they speak about." TikTok Br. 33. Indeed, the Act is utterly indifferent to who the speaker is or what the speech is. The Act is indifferent even as to whether the speech occurs on TikTok or a different platform, so long as the platform does not operate under the authority of the CCP. What the Act is *not* indifferent to is whether the

CCP has the ability to spy on Americans and then use their data against them. *See* Public Redacted Brief for Respondent at 66-67 ("The restriction on TikTok's ownership reflects the considered judgment of the political branches that China has the capability and incentive to use the application to amass massive amounts of U.S. user data and to exert covert influence over U.S. affairs in direct contravention of U.S. interests."). That reflects the government's longstanding and salutary approach to national security.

Similarly, the Act's naming of TikTok does not "single[] out TikTok for disfavor" or "punishment." *See* TikTok Br. 3, 61-68. Congress and the Executive Branch have routinely identified in legislation or regulation specific companies under China's control that pose particular national security risk. That is true for Huawei, ZTE, Dahua, Hikvision, and Hytera. *See supra*. In these other instances, just as with the Divestiture Act, Congress put in place a process for future designations in addition to naming particular threats. *See supra*. A practice that spans across many companies and reflects particular risk assessments does not single anyone out for punishment. The focus, rather, is on present risk based on a national security assessment made by members of Congress and the Executive Branch from different parties and different administrations.

As noted above, statutes and regulations of this kind have repeatedly been upheld by the courts. In *Huawei*, the Fifth Circuit sustained the FCC's designation

of Huawei and ZTE as covered companies. *Huawei*, 2 F.4th at 427. In *Hikvision v. FCC*, this Court rejected Hikvision and Dahua's challenge to the FCC's designation of their products on its list of covered equipment. *See* 97 F.4th at 944. And in 2020, a federal district judge directly rejected a bill-of-attainder challenge to the NDAA. *Huawei*, 440 F.Supp.3d. Despite naming Huawei, the NDAA did not impose "punishment." *Id.* at 630-50. "China is one of the leading threats" to the United States' cybersecurity, the court observed. *Id.* at 641 (cleaned). And addressing a national security threat in this way is a "legitimate regulation of conduct." *Id.* at 636. The same is true here.

When Congress legislates pursuant to its enumerated powers, it may advance any purpose not constitutionally prohibited. *See McCulloch v. Maryland*, 17 U.S. 316, 421 (1819) ("Let the end be legitimate, let it be within the scope of the Constitution, and all means which are appropriate, which are plainly adapted to that end, which are not prohibited, but consist with the letter and spirit of the Constitution, are Constitutional."). Indeed, the Constitution "entrust[s] the law making power to the Congress alone." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 589 (1952).

The Divestiture Act, which regulates TikTok's interstate and international commercial activity, is an unextraordinary exercise of Congress's lawmaking power. *See, e.g.*, U.S. Const. art. I, § 8, cl. 3 (foreign and interstate commerce powers), cl.

18 (Necessary and Proper Clause). Indeed, because the Act regulates domestic activity, it stands at the core of Congress's legislative power. *McCulloch*, 17 U.S. at 421; *see* Michael Ramsey, *The Constitution's Text in Foreign Affairs* 6 (2007) ("[A]ltering rights and duties within the domestic legal system, even in pursuit of foreign affairs objectives, … is a 'legislative' (lawmaking) function, not an executive one."). Congress's decision to determine that TikTok presents sufficient national security risk to require divestiture, rather than leaving that determination to executive judgment, does not offend our constitutional scheme.

CONCLUSION

The Court should deny the Petitions.

August 2, 2024

/s/ Thomas M. Johnson, Jr.
Thomas M. Johnson, Jr.
Jeremy J. Broggi
Michael J. Showalter
Stephanie Rigizadeh
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
Phone: (202) 719-7000
Fax: (202) 719-7049
tmjohnson@wiley.law
jbroggi@wiley.law
mshowalter@wiley.law
srigizadeh@wiley.law

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify, on August 2, 2024, that:

1. This document complies with the word limit under Federal Rule of Appellate Procedure 32(a)(7) because, excluding the parts of the document exempted by Federal Rule of Appellate Procedure 32(f), this document contains 6,493 words.

2. This document complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this document was prepared in a proportionally spaced typeface using Microsoft Word for Office 365 MSO in a 14-point Times New Roman font.

/s/ Thomas M. Johnson, Jr.
Thomas M. Johnson, Jr.

CERTIFICATE OF SERVICE

I certify that on August 2, 2024, a true and correct copy of this Brief of *Amici Curiae* was filed and served electronically upon counsel of record registered with the Court's CM/ECF system.

/s/ Thomas M. Johnson, Jr.
Thomas M. Johnson, Jr.